

## REMARKS

### **I. Introduction**

Claims 10, 11, and 14 to 18 remain pending in the present application. Claim 10 has been amended. In view of the foregoing amendments and the following remarks, it is respectfully submitted that all of the presently pending claims 10, 11, and 14 to 18 are allowable, and reconsideration of the pending claims is respectfully requested.

### **II. Rejection of Claims 10, 11 and 14-18 under 35 U.S.C. § 112, First Paragraph**

Claims 10, 11, and 14 to 18 were rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement.

Claim 10 has been rewritten to recite the phrase “during system operation subsequent to the previous, initial prompt/reply cycle,” thereby obviating the present rejection based on the phrase “during **normal** system operation.” Support for this amendment may be found in the Specification, *e.g.* at page 4, line 19 to page 5, line 11, which describes the system operation subsequent to the previous, initial prompt/reply cycle. Accordingly, it is respectfully submitted that claim 10 and its dependent claims 11 and 14-18 are in compliance with 35 U.S.C. § 112, first paragraph.

In view of all of the foregoing, withdrawal of this rejection is respectfully requested.

### **III. Rejection of Claims 10, 11, and 14-18 under 35 U.S.C. § 112, Second Paragraph**

Claims 10, 11, and 14 to 18 were rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention.

As discussed above, claim 10 has been rewritten to remove the term “normal” from the phrase “during **normal** system operation,” thereby obviating the present rejection. Accordingly, it is respectfully submitted that the present claims sufficiently “set forth and circumscribe a particular subject matter with a reasonable degree of clarity and precision,” which is all that is required under 35 U.S.C. § 112, second paragraph.

In view of the foregoing, withdrawal of this rejection is respectfully requested.

#### **IV. Rejection of Claims 10, 11 and 14-18 under 35 U.S.C. § 103(a)**

Claims 10, 11, and 14 to 18 stand rejected under 35 U.S.C. § 103(a) as unpatentable over the combination of U.S. Patent No. 5,745,576 (“Abraham”) and U.S. Patent No. 4,797,672 (“Kousa”). Applicants respectfully submit that this rejection should be withdrawn for the following reasons.

In rejecting a claim under 35 U.S.C. § 103(a), the Examiner bears the initial burden of presenting a *prima facie* case of obviousness. In re Rijckaert, 9 F.3d 1531, 1532, 28 U.S.P.Q.2d 1955, 1956 (Fed. Cir. 1993). In addition, as clearly indicated by the Supreme Court, it is “important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the [prior art] elements” in the manner claimed. See KSR Int’l Co. v. Teleflex, Inc., 127 S. Ct. 1727 (2007). To the extent that the Examiner may be relying on the doctrine of inherent disclosure in support of the obviousness rejection, the Examiner must provide a “basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic necessarily flows from the teachings of the applied art.” (See M.P.E.P. § 2112; emphasis in original; see also Ex parte Levy, 17 U.S.P.Q.2d 1461, 1464 (Bd. Pat. App. & Inter. 1990)).

Amended claim 10 recites the following:

10. A system for access authorization, comprising:

a base device including a computer, wherein the base device initially transmits a prompt signal within a framework of an initial prompt/reply cycle that is successfully carried out, and wherein the prompt signal is stored in the base device; and

at least one remote control storing the initially transmitted prompt signal from the initial prompt/reply cycle;

wherein, **in an access authorization process during system operation subsequent to the previous, initial prompt/reply cycle that is successfully carried out**, the at least one remote control transmits to the base device a code word containing a reply, **the reply being formed at least partially as a function of the prompt signal stored in the at least one remote control**, wherein the base device receives the code word containing the reply and compares the reply contained in the code word with a required reply, **the required reply being formed at least partially as a function of**

**the prompt signal stored in the base device**, wherein an access is authorized if the reply contained in the code word agrees with the required reply, and wherein **the prompt signal stored in the base device is erased when a number of failed agreements of the reply and the required reply exceeds a specifiable limiting value.**

Support for these amendments may be found in the Specification, e.g. at page 4, lines 32 to 33.

In contrast, Abraham does not disclose, or even suggest, all of the claimed features of claim 10, as presented. The Office Action admits that “Abraham does not disclose that an initial stored prompt from a successful prompt/reply cycle is used to encrypt the authorization information.” (Office Action, p. 3). Thus, Abraham plainly does not disclose, or even suggest, the feature that in an access authorization process during system operation subsequent to the previous, initial prompt/reply cycle that is successfully carried out, the at least one remote control transmits to the base device a code word containing a reply, the reply being formed at least partially as a function of the prompt signal stored in the at least one remote control, as provided in claim 10. Furthermore, Abraham also does not disclose, or even suggest, the feature that the base device receives the code word containing the reply and compares the reply contained in the code word with a required reply, the required reply being formed at least partially as a function of the prompt signal stored in the base device, as provided in claim 10. Abraham explicitly states that “[t]he base [or initial] key is used only for the purposes of initialization of cryptographic terminals, and is not used for normal [system] operations.” (Abraham, Abstract; col. 5, lines 16 to 18; and col. 5, lines 25 to 26). In this regard, Abraham further states that following initialization, “the controller can provide … the operational key to be used by the terminal for transactions between the controller and the new terminal.” (Abraham, col. 7, lines 45 to 50). Contrary to the “Response to Arguments” at page 5 of the present Office Action stating that “initialization is a normal system operation,” Abraham makes a clear distinction between initialization and normal system operations, by clearly indicating an initial base key for initialization purposes, and a distinct, operational key for use during normal system operations. Thus, since Abraham does not use the prompt signal stored in the remote control to form the reply during system operation, Abraham also does not use the prompt signal stored in the base device to form the required reply during system operation. Furthermore, since the Office Action admits that “[w]ith regard to the base computer erasing the session

key after a number of failed attempts, Abraham does not mention abandoning the process after a specific number of failed attempts,” (Office Action, p. 4), Abraham does not disclose, or even suggest, the feature that **the prompt signal stored in the base device is erased when a number of failed agreements of the reply and the required reply exceeds a specifiable limiting value**, as provided in claim 10.

In addition to the above, although the Examiner states that “Kousa discloses that often an encrypted exchange will be preceded by a key exchange to create a session key to use in further authentications,” it is respectfully submitted that Kousa fails to cure the critical deficiencies of Abraham with respect to all of the claimed features of claim 10. Kousa explicitly states that “[t]he node encryption key is used only at the beginning of a communication sequence” in which the base station generates an encrypted, random number and transmits it to a node station, which then decrypts the random number and uses it as a “seed” for generating more random numbers. Then, the node station generates its own encrypted, random number, which the base station decrypts and uses as a “seed” for encrypting messages sent to the node station. (Kousa, col. 2, lines 26 to 45). Therefore, Kousa clearly does not disclose, or even suggest, the feature that in an access authorization process during system operation subsequent to the previous, initial prompt/reply cycle that is successfully carried out, the at least one remote control transmits to the base device a code word containing a reply, the reply being formed at least partially as a function of the prompt signal stored in the at least one remote control, as provided for in the context of claim 10, as presented. The node station of Kousa merely uses its “seed” to form its reply to the base station, but does not form the reply at least partially as a function of the node encryption key. Furthermore, Kousa clearly does not disclose, or even suggest, the feature that the base device receives the code word containing the reply and compares the reply contained in the code word with a required reply, the required reply being formed at least partially as a function of the prompt signal stored in the base device, as provided in claim 10. The base station of Kousa also uses its “seed” to form encrypted messages to the node station, but does not form the required reply at least partially as a function of the node encryption key. Significantly, the base station “seed” is initially generated by the node station, not the base station itself, and the respective “seeds” of the base station and the node station are distinct from each other. In addition, Kousa does not disclose, or even suggest, the feature that **the prompt signal stored in the base device is erased when a number of failed agreements of the reply and the required reply exceeds a specifiable limiting value**, as

provided in claim 10. Therefore, the proposed combination of Abraham and Kousa does not disclose, or even suggest, all of the claimed features of claim 10.

In addition to the above, to the extent the Examiner additionally cites See (U.S. Patent No. 6,070,243) and Schneier (Applied Cryptography) in the discussion of the rejection nominally based on Abraham and Kousa, Applicants note that See and Schneier fail to cure the critical deficiencies of the proposed combination of Abraham and Kousa with respect to all of the claimed features of claim 10. See merely indicates terminating a session with a user after a predetermined number of failed login attempts, and Schneier merely indicates erasing session keys when a session is ended. However, neither See nor Schneier discloses, or even suggests, the features that in an access authorization process during system operation subsequent to the previous, initial prompt/reply cycle that is successfully carried out, the at least one remote control transmits to the base device a code word containing a reply, the reply being formed at least partially as a function of the prompt signal stored in the at least one remote control; the base device receives the code word containing the reply and compares the reply contained in the code word with a required reply, the required reply being formed at least partially as a function of the prompt signal stored in the base device; and the prompt signal stored in the base device is erased when a number of failed agreements of the reply and the required reply exceeds a specifiable limiting value, as provided in claim 10. Neither See nor Schneier discloses, or even suggests, the features of the prompt signal, the reply, and the required reply, as provided in claim 10. Therefore, See and Schneier fail to cure the critical deficiencies of the proposed combination of Abraham and Kousa.

Accordingly, for at least the foregoing reasons, the proposed combination of Abraham and Kousa does not render unpatentable claim 10 and its dependent claims 11 and 14-18.

In view of all of the foregoing, withdrawal of this rejection is respectfully requested.

**CONCLUSION**

Applicants respectfully submit that all pending claims of the present application are now in condition for allowance. Prompt reconsideration and allowance of the present application are therefore earnestly solicited.

Respectfully submitted,



(R.N.O.  
36,197)

Dated: June 3, 2008

By: Jong Lee for Gerard Messina  
Gerard A. Messina  
Reg. No. 35,952

KENYON & KENYON LLP  
One Broadway  
New York, New York 10004  
(212) 425-7200

**CUSTOMER NO. 26646**